a program memory in which the secure program data is stored in an encrypted form;

a security chip coupled between the program memory and adapted to be coupled to a processor over an accessible processor bus, the security chip comprising:

means for decrypting portions of the secure program into a clear portion and a remainder portion;

means for providing the clear portion to memory locations accessible by the processor; and

remainder memory for storing the remainder portion of the secure program, the remainder memory not directly accessible by the processor except via the security chip;

means for requesting subsets of the remainder portion for use by the processor; and

means, within the security chip, for checking that the requested subset is within a valid predetermined set of ~~a validly~~ requested subsets given a stored state for the processor.--

REMARKS

Claims 2, 5-6, 8-9, 12, 17, 20-23, 25-27, 29-30 and 32 are hereby amended and new claim 33 is herein submitted for entry and examination. Therefore, claims 1-33 are currently pending in the present application.

Claims 1-32 stand rejected under 35 USC §112, ¶2, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-32 also stand rejected under 35 USC §103 as being unpatentable over Arnold (U.S. Patent No. 4,558,176 issued to Arnold et al.), Gaffney (U.S. Patent No. 4,562,305 issued to Gaffney Jr.) or Ogura (U.S. Patent No. 5,544,244).

42

Rejection under §112

The Examiner rejected all the claims under §112, ¶2 stating that a number of descriptive terms used in the claims were not positive limitations and hence ambiguous. Applicants note that the Office Action did not specify which language in which claims was found objectionable. The Office Action listed some language that was found objectionable, but the claims in which any one of the objectionable terms can be found is less than all the claims, thus the rejection of all the claims is improper or incomplete. To the extent that the objections are understood, the claims have been amended to overcome the §112 rejection, except where the objections are herein traversed. Applicants have also made several additional amendments to the claims to clarify the scope of the claims. No change in the scope of the claims is intended thereby.

Applicants respectfully traverse the Examiner's objection to claim 1, as the language "expected to be requested" is a positive limitation and does not depend on future acts. In the context of the limitation where the language appears, a means for checking is recited which checks the requested subset. The claimed computer system can operate in a normal, expected manner, or it can be modified by an attacker bent on reverse engineering the secure program. If a processor's state determines which subset could be requested and the processor is operated normally, the subset which will be requested given a state for the processor can be predicted, i.e., it is the subset which is "expected to be requested" given the stored state. In some cases, more than one subset could be validly requested for a given state, but the subset that is actually requested is one that is expected to be requested.

If a state is stored for the processor, then an expected subset (or a group of expected subsets to select from) will be known. If the processor is operating as expected (e.g., not being reverse engineered), the means for checking will find that the requested subset is one that can be expected to be requested. However, if the processor is not operating as expected (e.g., it is being controlled in an attempt to extract the secure program data in an unencrypted form), then it is likely that a subset other than an expected subset will be requested. In the latter case, the means for checking will detect that the requested subset is not a subset expected to be requested given a stored state for the processor.

In either case, the language of the limitation of a means for checking does not require a future act and is a positive limitation in that it limits what the requested subset is checked against. Having addressed the rejection, Applicants respectfully request withdrawal of the rejection under 35 USC §112, ¶2.

Rejection Under §103

The Claimed Invention:

The present invention is directed to a method and apparatus for securing programs. In one embodiment, a security chip is provided as an interface between a program memory containing a secure program and a processor. The secure program in the program memory is secure because it is encrypted. To actually execute the program on the processor, the program needs to be decrypted. If the program were simply decrypted in its entirety, then copying the program without needing to duplicate the security chip would be simple. To prevent this, the security chip only provides subsets of a remainder portion to the processor (a clear portion of the secure program is provided in memory locations accessible by the processor).

The Cited References:

Arnold (U.S. Pat. No. 4,558,176 issued to Arnold, et al.) discloses a security system where programs are decrypted only inside a security CPU enclosed in an impenetrable form. (see column 4, lines 28-33)

Gaffney (U.S. Pat. No. 4,562,305) discloses encrypting object code so as to enable relocation of that code.

Ogura (U.S. Pat. No. 5,544,244) discloses a method for protecting computer object code where extra ignored instructions are included in the object code to make decoding more difficult.

The Cited References Distinguished:

Claim 1, as amended, recites a security chip which is not disclosed or suggested in any of the cited references. In the Office Action, the Examiner did not cite where in the cited references each element of claim 1 could be found. The Examiner did, however, generally cite columns 20, 61 and 65 of Arnold, Fig. 1 of Gaffney and Figs. 7-8 of Ogura against all of the claims. However, in a review of those citations, a disclosure or suggestion was not found of a security chip with a means for decrypting portions of a secure program into a clear portion and a remainder portion, a remainder memory for storing the remainder portion not directly accessible by a processor, and a means for checking requested subsets, among other claimed elements.

Column 20 of Arnold appears to be directed to a method of detecting illegal tampering in a system where an encrypted program is executed by a security CPU where a key is destroyed when a branch out of bounds occurs. While this deals with branching and some of Applicants' claims (but not claim 1) recite branches and the separation of branch instructions from nonbranch instructions, it is not apparent how column 20 of Arnold applies to the present claims.

The marked portions of column 61 of Arnold are directed to how bytes on a bus are decrypted. Apparently, Arnold provides for separate treatment of bytes on the bus. If a byte is an instruction field, one cipher is used, if it is an operand field another cipher is used, and if it is an address field of a branch instruction the address is decrypted as a unit instead of one byte at a time. The relevance of this to the present invention is not understood. Column 65 of Arnold also deals with branches, among other topics, but its relevance is not understood, either to Applicants' claims which do not recite branches or those which do.

Similarly, the relevance of Gaffney and Ogura is not understood. Therefore, the Examiner has not made a *prima facie* showing that claim 1 is unpatentably obvious over the cited references, and the rejection under §103 should either be withdrawn or the Examiner should point out where in the cited references each of the claimed limitations or their obvious counterparts can be found.

A *prima facie* showing has also not been made out with respect to claims 2-32.

The showing for claims 2-18 fails for the reasons stated above in addition to the lack of a showing of the additional limitations recited in those claims.

As for claim 19, no *prima facie* showing was made that the claimed branch separator, compressor and encryptor are disclosed or suggested in the cited references. Gaffney may be related to differential treatment of branch instructions vs. nonbranch instructions in that branch instructions are decrypted such that they are relocatable, but this is not relevant to claim 19, as claim 19 recites a branch separator. If Gaffney had used a branch separator, his instruction P2 would not be stored in program store 4 with all the other instructions P0-P1, P3-P7 (see Fig. 1 of Gaffney). Ogura likewise provides for differential processing of branch instructions, but the instructions appear to be all stored in one place, namely external memory 50 (see Figs. 7-9 of Ogura). Therefore, claim 19 is allowable over the cited references.

For similar reasons, claims 20-32 are allowable over the cited references.

For the reasons set forth above, Applicants respectfully assert that claims 1-32 are allowable over the cited art and request that the rejection under §103 be reconsidered.

CONCLUSION

The undersigned believes that this amendment is responsive to each of the objections and rejections made in the Office Action and that they have been overcome for the reasons set forth in the remarks. Reconsideration and allowance of all pending claims is earnestly solicited. If it is deemed that a telephone conversation would expedite the prosecution of the present application, the Examiner is invited to call the undersigned attorney at (415) 576-0200.

Respectfully submitted,

Date: 3 DEC 96

By
Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, CA 94111-3834

Telephone: (415) 576-0200
Fax: (415) 576-0300